Nihal Taşcı
2264687

CENG435
WSA6

```
nihal@makine:~$ ping -c 10 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=55 time=26.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=55 time=23.7 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=55 time=24.0 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=55 time=24.2 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=55 time=24.0 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=55 time=26.9 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=55 time=23.8 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=55 time=24.0 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=55 time=23.9 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=55 time=23.9 ms

--- 8.8.8.8 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9012ms
rtt min/avg/max/mdev = 23.702/24.517/26.926/1.141 ms
nihal@makine:~$ ip route
default via 192.168.1.1 dev wlp3s0 proto dhcp metric 600
169.254.0.0/16 dev wlp3s0 scope link metric 1000
192.168.1.0/24 dev wlp3s0 proto kernel scope link src 192.168.1.227 metric 600
```

Answers:

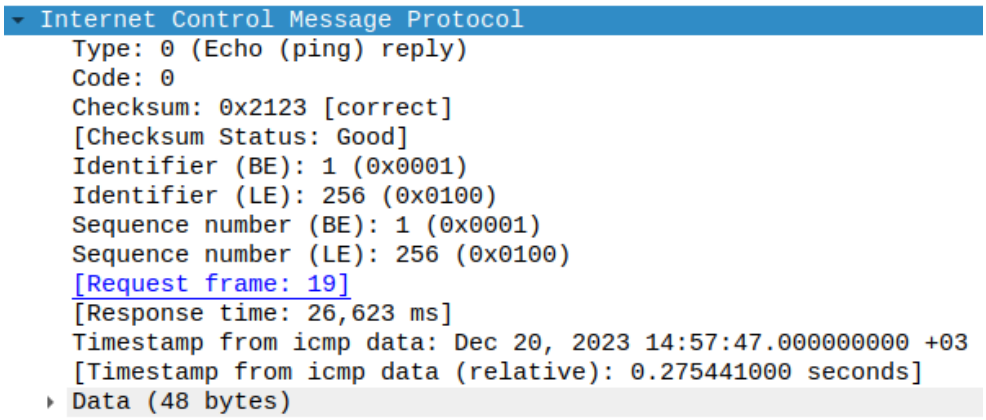
1.

icmp

No.	Time	Source	Destination	Protocol	Le
19	2.058924	192.168.1.227	8.8.8.8	ICMP	
20	2.085547	8.8.8.8	192.168.1.227	ICMP	
29	3.060362	192.168.1.227	8.8.8.8	ICMP	
30	3.084037	8.8.8.8	192.168.1.227	ICMP	
39	4.062430	192.168.1.227	8.8.8.8	ICMP	
42	4.086308	8.8.8.8	192.168.1.227	ICMP	
59	5.063490	192.168.1.227	8.8.8.8	ICMP	
60	5.087630	8.8.8.8	192.168.1.227	ICMP	
203	6.064948	192.168.1.227	8.8.8.8	ICMP	
204	6.088958	8.8.8.8	192.168.1.227	ICMP	
213	7.066423	192.168.1.227	8.8.8.8	ICMP	
214	7.093222	8.8.8.8	192.168.1.227	ICMP	

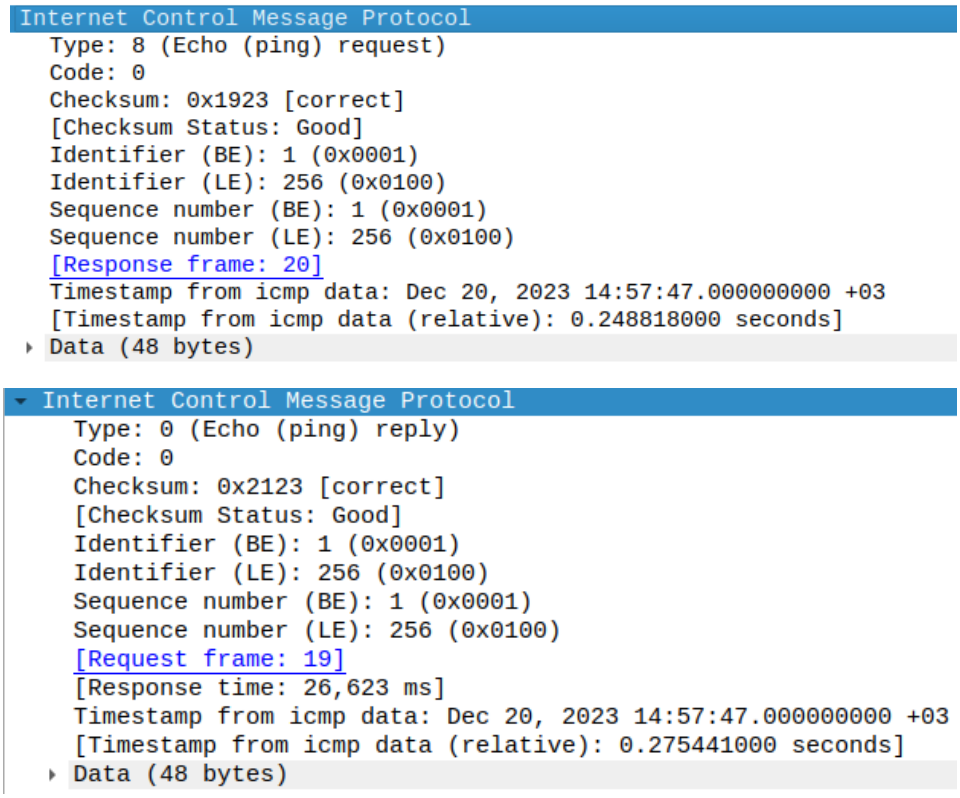
For the request packets, the source host is 192.168.1.227 and the destination host is 8.8.8.8.
For the reply packets, the source host is 8.8.8.8 and the destination host is 192.168.1.227.

2.



No, there is not any port number information in these packets. The reason is that ICMP is a network layer protocol and established between hosts not processes, so it does not need port numbers.

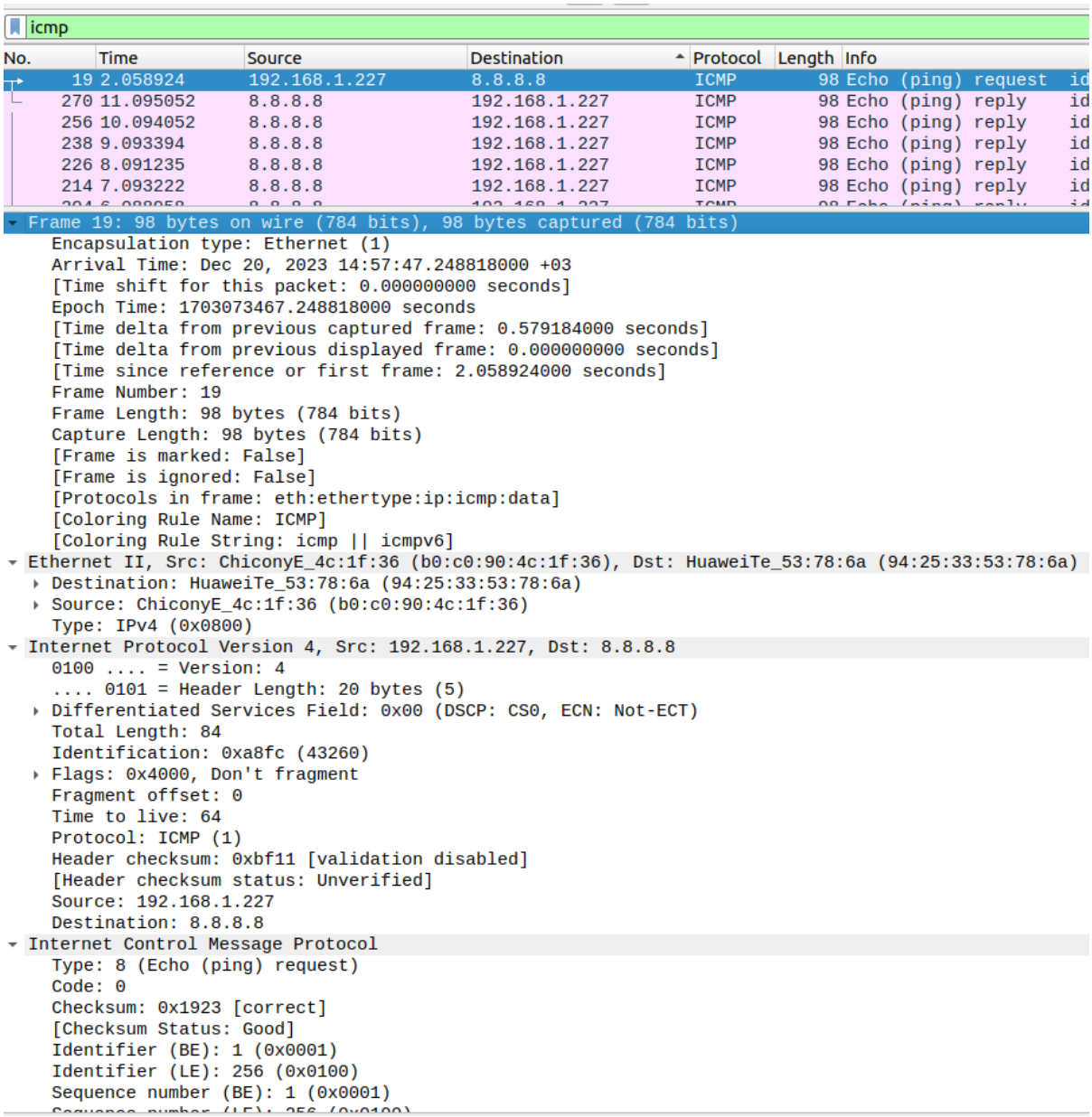
3.



a. The purpose of the type field is to specify the type of the ICMP packet, such as request or response. The values represent different situations, for example 8 means echo ping request and 0 means echo ping reply on the screenshot.
b. The purpose of the code field is to provide specific details for a control message of the type determined by the type field, for example 0 means no problem or 3 means destination unreachable situation.

c. For request, the type field being 8 means echo request (ping request) and the code field being 0 for it means that the specific ICMP message is a basic echo request without any further specific details.
For reply, the type field being 0 means echo reply (ping reply) and the code field is typically set to 0 and it means the specific ICMP message is a basic echo reply without any further specific details.

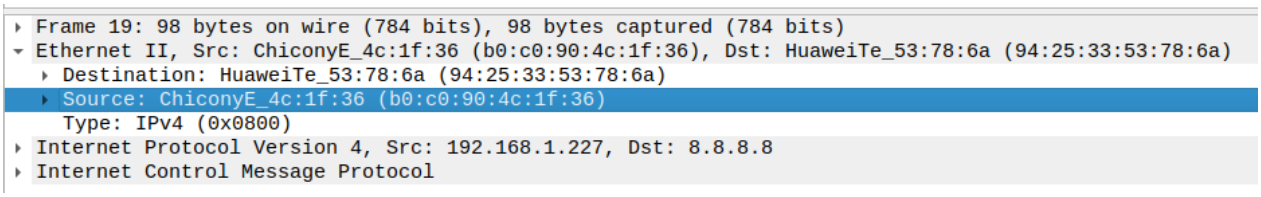
4.



By looking at the ICMP request packet information, 98 bytes are transferred in total.
20 bytes for IP header
48 bytes for data
14 bytes for Ethernet protocol header
16 bytes for ICMP header (1 byte for packet type, 1 byte for packet code, 2 bytes for checksum, 2 bytes for identifier, 2 bytes for sequence number, 8 bytes for timestamp data.)

5. To prevent outgoing packets and sending ping requests, I should remove the default gateway rule. I can use this command:
sudo ip route del default via 192.168.1.1 dev wlp3s0
With this command, I can remove the default gateway and my machine cannot send any ping requests anymore.

6.



a. The 48-bit Ethernet address of my computer is b0:c0:90:4c:1f:36.
b. The 48-bit destination address in the Ethernet frame is 94:25:33:53:78:6a. This Ethernet address belongs to a Huawei device which is a router.
c. During the packet capture, I encountered the value in the type field in Layer 2:
0x0800: IPv4
So, the Ethernet frames are carrying IPv4 packets.